Licence professionnelle *Réseaux et Sécurité*
Projets tutorés 2012-2013

Sujets proposés à l'Université de Cergy-Pontoise

1. Déploiement d'une architecture téléphonique hybride : PC-Asterisk/PABX analogique, CISCO et Panasonic + annuaire et proxy (3 élèves)

Tuteurs : *Frédéric Wrobel,* frederic.wrobel(à)u-cergy.fr*, Tuyêt Trâm Dang Ngoc***,** dntt(à)u-cergy.fr

Le but de ce projet est de déployer la téléphonie sur IP et analogique sur un site puis de l'interconnecter avec un autre site

a. Site 1

- Création d'un autocommutateur analogique

Vous disposez d'un PC contenant les deux cartes suivantes Digium TDM31B TDM PCI Card (3FXS-1FXO). Sur chacune de ces cartes, vous pouvez relier sur les ports FXS, un périphérique analogique FXO (téléphone, fax, etc.) et sur les ports FXO une liaison vers un port FXS.
Le logiciel Asterisk permet de transformer un tel PC en un autocommutateur PABX. Dans cette première étape, vous créerez un autocommutateur sur ce PC.
Pour cela :

- Vous installerez et configurerez Asterisk afin de prendre en charge les ports FXS.
- Vous attribuerez à votre autocommutateur le préfixe 0123 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

- Création d'un d'un réseau téléphonique IP

Vous disposez d'un autre PC ne possédant pas de cartes dédiées à la téléphonie (pas de FXS ou FXO), simplement une carte réseau Ethernet. Il s'agit ici de réaliser un PBX entièrement basé sur IP. La téléphonie sur IP s'appuie sur le protocole SIP.

- Vous mettrez en place le réseau 192.168.42.0/24 sur lequel vous connecterez votre PBX IP ainsi que deux autres PC.
- Vous créerez des lignes SIP 2000, 2001, 2002, etc. que vous attribuerez aux téléphones IP. Vous utiliserez plusieurs types de téléphones IP : un téléphone IP filaire, un téléphone IP wifi, un softphone comme ekiga + casque et micro, un téléphone USB
- Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur IP.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.
- Mettez en place et expérimentez au maximum les services offerts par Asterisk : présentation du nom, filtrage d'appel, etc.

- Création de la passerelle analogique
  - Reliez votre PC commutateur analogique au réseau IP construit dans la section précédente.
  - Faites en sorte que les téléphones IP puissent appeler les téléphones analogiques du réseau RTC et vice-versa.

b. Site 2

- Utilisation d'un autocommutateur analogique propriétaire

  Vous disposez d'un PABX/IPBX propriétaire Panasonic permettant le déploiement d'un réseau téléphonique analogique/numérique.

- Vous attribuerez à votre autocommutateur le préfixe 0145 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques et de téléphones numériques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

- Création d'un d'un réseau téléphonique IP
  Vous créerez un PBX entièrement basé sur IP en utilisant les équipements CISCO dédiés à cet effet,

c. Interconnexion de sites

- Connexion IP à IP : Réalisez l'interconnexion entre les réseaux téléphoniques IP avec l'autre site.
- Connexion RTC à RTC : A l'aide des ports FXO, réalisez l'interconnexion entre les réseaux analogiques des deux sites.

d. Fonctionnalités supplémentaires

- Utilisation de proxy et de redirecteur pour la téléphonie IP : Mettez en place un proxy et un redirecteur permettant l'enregistrement des numéros et (jabber) téléphone dans un intranet. Cette fonctionnalité est importante par rapport à l'évaluation finale du projet.
- Intégration LDAP : Vous déploierez et utiliserez un annuaire LDAP pour les services de présentation du nom, recherche numéro, etc.
- Visio-conférence: Sur votre machine Asterisk, prenez en compte le protocole H323 afin de permettre la visio-conférence. Testez.
- Modem : Un numéro de téléphone sur un des sites devra également être disponible afin de pouvoir être appelé en utilisant le réseau RTC et permettre une connectivité IP par ce biais.
- Fax : Un numéro de fax devra être offert et utilisable.

Travail demandé
Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme téléphonique qui devra être fonctionnelle, maintenable et redéployable. Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les pré-requis et les concepts notamment de téléphonie ainsi que les difficultés rencontrées, les remarques et les limitations. Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

2. Plate-forme de travail collaboratif : eSupPortal, LDAP, Serveur CAS (3 élèves)

Tuteur : *Marc Lemaire,* marc.lemaire(à)u-cergy.fr

Le but de ce projet est de réaliser la mise en place d'un ENT (environnement numérique de travail).

Dans le cadre du déploiement d'un espace numérique de travail (ENT), il s'agit de pouvoir permettre aux utilisateurs répertoriés dans un annuaire LDAP, un accès à différents services.

L'utilisateur doit pouvoir être identifié qu'une seule fois (SSO - Single Sign On) auprès d'un serveur CAS (Central Authentfication Service) lors de son premier accès à un des services. Par la suite, une fois l'utilisateur identifié et authentifié, celui-ci aura accès -sans authentification supplémentaire- à l'ensemble de son espace numérique de travail.

Celui-ci doit obligatoirement comporter les services suivants :

- configuration du profil utilisateur
- accès à sa boite aux lettres
- un espace de stockage pour gérer ses documents
- un calendrier
- une gestion de ses pages web
- didacticiel (moodle)

Une interaction avec les autres utilisateurs doit également être possible :

- partage de fichiers
- chat et messagerie
- forum

Vous pourrez à cette fin, utiliser les solutions libres OpenPortail/eSupPortail avec ses nombreux portlets.

Son objectif premier est de fournir un espace numérique de travail modulaire, avec un accès unique et ergonomique à différents services et diverses sources d'informations et ressources numériques.

Travail demandé
Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme ENT qui devra être fonctionnelle, maintenable et redéployable.

Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les prérequis et les concepts notamment d'authentification SSO ainsi que les difficultés rencontrées, les remarques et les limitations.

Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

3. <u>Domaine Active Directory, DMZ, RADIUS, routeur et FTP</u> (2-3 élèves)

Tuteur : *Guillaume Renier,* guillaume.renier(à)u-cergy.fr

Contexte
Une entreprise dispose d'un réseau local, d'une DMZ et est connecté à l'internet par l'intermédiaire d'un routeur. Un domaine AD est présent et configuré pour l'entreprise. Les contrôleurs sont accessibles uniquement sur le réseau local de l'entreprise. Chaque employé de l'entreprise dispose d'un compte sur le domaine AD.

Il est possible d'ouvrir des ports de la DMZ vers le réseau local (et donc les contrôleurs de l'AD).

Présentation
L'entreprise veut installer un serveur FTP dans la DMZ qui authentifiera les utilisateurs par l'intermédiaire de l'AD. Ce serveur doit créer dynamiquement un répertoire personnel pour chaque utilisateur.

Objectifs
Les contrôleurs AD 2008S peuvent être configurés en lecture seule. Les ouvertures de ports entre la DMZ et le réseau local ne se feront que vers un contrôleur 2008S en lecture seule. Le réseau local dispose donc d'au moins trois contrôleurs W2008S dont au moins 1 est en lecture seule et au moins 2 sont en lecture/écriture.

Le serveur FTP doit être un logiciel libre au sens large du terme. Il doit être installé sur un serveur UNIX (linux, FreeBSD, macOS...) et utiliser une authentification par PAM.

PAM doit être configuré pour utiliser :
- Soit un module pour RADIUS qui sera configuré pour utiliser un serveur RADIUS sur le serveur 2008.
- Soit un module LDAP qui sera configuré pour se connecter sur l'AD du serveur en lecture seule.

Le serveur FTP doit pouvoir être utilisé depuis l'internet et depuis le réseau local.

Les étudiants devront configurer 5 serveurs : 1 contrôleur 2008S en lecture/écriture, 1 contrôleur 2008S en lecture seule, 1 routeur (matériel ou logiciel) et un serveur UNIX. Le tout pouvant se faire sur des systèmes virtualisés.

Extension possible
La connexion sur le serveur FTP pourra se faire en SFTP ou en FTPS.

La connexion sur les répertoires personnels sur le serveur FTP pourront être accessible en NFS, CIFS depuis le réseau local.

4. <u>Domaine Active Directory, VLAN, serveur RADIUS, 802.1X, routeur, firewall, proxy filtrant</u> (2-3 élèves)

Tuteur : *Guillaume Renier,* guillaume.renier(à)u-cergy.fr

Contexte

Une entreprise dispose d'un réseau local et est connecté à l'internet par l'intermédiaire d'un routeur / firewall. Un domaine AD est présent et configuré pour l'entreprise. Les contrôleurs sont accessibles uniquement sur le réseau local de l'entreprise. Chaque employé de l'entreprise dispose d'un compte sur le domaine AD.

Les employés sont
– Soit des cadres.
– Soit des non-cadres

Présentation

L'entreprise souhaite accorder des droits d'accès à internet en fonction du statut (cadre / non cadre) des employés. Les cadres doivent disposer d'un accès complet à internet avec filtrage des sites web par liste noire. Les non cadres doivent disposer d'un accès à internet limité par liste blanche.

Pour cela, elle souhaite mettre en place une authentification 802.1X avec affectation dynamique de VLAN (il est possible d'imposer la marque du matériel actif utilisé.)
Le VLAN 3 sera réservé aux cadres et le VLAN 4 aux non-cadres.
Le VLAN 1 sera réservé à la gestion des switchs.
Le VLAN 2 sera réservé aux serveurs.
Le routeur assurera du routage interVLAN (3--2 et 4--2). Les VLAN 3 et 4 seront cloisonnées.
Le filtrage des sites web se fera en fonction du VLAN : le routeur pourra rediriger de manière transparente les accès web (port 80) sur un proxy squid configuré pour utiliser des redirecteurs squidGuard (le filtrage des sites web ne se fait donc pas en fonction du nom utilisateur).

L'authentification 802.1X utilisera un serveur RADIUS qui authentifiera grâce à un annuaire LDAP.
L'annuaire LDAP sera au choix : l'AD des contrôleurs de domaine ou un OpenLDAP.
Néanmoins les comptes utilisateurs seront créés sur un AD.
Dans le cas d'un openLDAP il sera nécessaire de procéder à une réplication d'une partie de l'AD dans le LDAP (on pourra dans un premier temps utiliser un annuaire LDAP configuré spécifiquement).

Objectifs

Configurer l'ensemble des serveurs et des switchs.
Configurer l'ensemble des routeurs / firewall, proxy (on pourra utiliser une distribution IP-COP).

Extension possible

On pourra faire en sorte que cette authentification fonctionne avec des postes Windows accrochées au domaine (avec donc une ouverture de session sur le domaine).

Sujets proposés à l'EPMI

5. Mise en place d'une infrastructure de sécurité de Haute disponibilité (3 élèves)
Tuteur *Nabil Ouassini*, n.ouassini(à)epmi.fr

En utilisant la technologie LVS sous linux vous devez mettre en place une infrastructure de sécurité sur laquelle repose un cluster de serveurs WEB.

A titre d'exemple vous hébergerez l'application OpenERP et prouverez que les modifications sont répercutées sur tous les serveurs de votre grappe.

Vous disposerez de 3 PC physiques DualCore pour émuler des serveurs de production.

Vous démontrerez que votre choix de type de LVS est le plus pertinent.

Vous devrez expliquer et documenter la technologie LVS.

6. Création d'une architecture de production pour environnement de développement WEB (3 élèves)
Tuteur *Alex Falzon*, a.falzon(à)epmi.fr

Afin de permettre à une équipe de développeur de travailler dans un environnement hétérogène maitrisé, vous allez mettre en place une architecture comprenant :

- Un serveur de sauvegarde intégrant la gestion des VPN SSH avec Certificats jusqu'au serveur WEB et un mécanisme de sauvegarde par cycle sous Windows 2008 srv.
- Un serveur apache et MySQL de production sous Debian.
- Un serveur apache et MySQL de pré-production sous Debian.
- 2 stations de travail.

La gestion des sauvegardes et (fichiers et bases) doit être centralisé sur l'infrastructure MICROSOFT.

La gestion des mise en production des fichiers sur le serveur de production devra être effectué par lancement de script via un tunnel direct entre les 2 serveurs.

Vous disposerez de

- 3 PC physiques pour émuler des serveurs.
- 1 Switch et 1 routeur pour émuler le WAN
- 2 stations de travail.
- 1 Switch et 2 routeurs.

Vous devrez expliquer et documenter les technologies OpenVPN et SSH ainsi que la mise en place des scripts et/ou outils de sauvegarde choisis.

7. **Sécurisation centralisée (2 élèves)**
   Tuteur *Alex Falzon,* a.falzon(à)epmi.fr

Afin de sécuriser son site, une société à opté pour la mise en place d'un cluster de firewall PFsense avec les fonctionnalités suivantes :

Un mécanisme de load-balancing doit être déployé sur 2 sorties WAN.

Du fail-over doit être déployé sur le cluster.

Une DMZ devra être présente.

Un portail captif sera déployé pour le réseau invité WIFI en s'appuyant sur RADIUS

Le radius sera implémenté avec Freeradius dans l'OS de votre choix, mais virtualisé sous Débian.

Vous disposerez de

- 1 serveur lame Dell octocore.
- 1 point d'accès WIFI.
- 1 Switch et 2 routeurs.
- 2 stations de travail.

8. **Sécurisation d'un environnement de virtualisation et stockage de donnés (2 élèves)**
   Tuteur *Nabil Ouassini,* n.ouassini(à)epmi.fr

Vous allez installer un cluster de serveurs ProxMox s'appuyant sur une authentification Radius.

Le stockage se fera sur un SAN NetApps en RAID.

La totalité des authentifications d'équipements actifs devra être gérée par une authentification 802.1x centralisée.

Un mécanisme de haute dispo devra être déployé sur le cluster avec DRDB.

Une connexion du SAN en iSCSi sur chacun des 2 hyperviseurs avec synchronisation DRBD.

- 2 serveurs lame Dell octocore.
- Un SAN Netapps.
- 1 Switch et 1 routeur.
- 2 stations de travail.

Sujets proposés par les élèves

9. Optimisation de la gestion des stations étudiantes (3 élèves)

Tuteurs : *Alex Falzon*, a.falzon(à)epmi.fr

Mise en place d'une solution Virtual Desktop Infrastructure (VDI) sur Windows Serveur 2012.
La mise en place de cette technologie offre un environnement de travail (en "clients légers") comprenant :
De la virtualisation avec l'installation de Windows Serveur 2012 sur un serveur ProxMox
De l'identification (gestion AD)
Un fonctionnement à la manière d'un compte itinérant (sauvegarder les données du bureau virtuel)
La mise en place de web-apps

Vous disposerez de

- 1 serveur lame Dell octocore.
- 1 point d'accès WIFI.
- 1 Switch et 2 routeurs.
- 2 stations de travail.

.